



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,491	11/14/2005	Heikki Waris	884A.0093.U1(US)	9069
29683 7590 05/11/2009 HARRINGTON & SMITH, PC 4 RESEARCH DRIVE, Suite 202 SHELTON, CT 06484-6212				
EXAMINER				
LEE, ANDREW CHUNG CHEUNG				
ART UNIT		PAPER NUMBER		
2419				
MAIL DATE		DELIVERY MODE		
05/11/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/531,491

Applicant(s)

WARIS, HEIKKI

Examiner

Andrew C. Lee

Art Unit

2419

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 April 2009.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 and 22-36 is/are pending in the application.
4a) Of the above claim(s) 19-21 is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-18, 22-34 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-8508)
Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. Claims 19 – 21 have been canceled.

Claims 35, 36 are newly added.

Claims 1 – 18, 22 – 36 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1 – 13, 15, 17 – 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kakemizu et al. (US 20020018456 A1) and Lee et al. (US 20020085517 A1) in view of Balaz et al. (US 20060179298 A1).

Regarding claim 1, Kakemizu et al. disclose a network (*Fig. 1, Fig. 2, Fig 4*) comprising: an internal secured portion ("*VPN of IP sec.*" interpreted as *internal secured portion*; *Fig. 2, para [0017], Fig. 25, para [0113]*), except a virtual private network certificate authority; an external portion ("*public IP network*" interpreted as *an external portion*; *Fig. 2, para [0017], Fig. 25, para [0113]*); at least one mobile node in the external portion element ("*MN 1*" interpreted as *at least one mobile node in the external portion*; *paragraph [0017]*); at least a first gateway (*Fig. 2, "element 21 VPNGW(FA)" interpreted as the first gateway*; *paragraph [0017]*); and at least a second gateway ("*element 31 VPNGW(HA)*"

Art Unit: 2419

interpreted as a second gateway), where the internal secured portion connects via the first gateway and the second gateway to the external portion (Fig. 2, Fig. 4, *VPN of IP sec.*” *interpreted as internal secured portion*, “*element 21 VPNGW(FA)*” *interpreted as the first gateway*, (“*element 31 VPNGW(HA)*” *interpreted as a second gateway*; Fig. 2, para [0017], Fig. 25, para [0113], and the network is configured to change the gateway, which the mobile node uses to communicate with the internal secured portion, from the first gateway to the second gateway in response to movement of the mobile node (*paras.*[0113], [0119] – [0121])). Kakemizu et al. also disclose care-of-address (*para. [0100]*).

Kakemizu et al. do not disclose explicitly in response to a receipt from the mobile node of a new care- of-address that is different from a first care-of-address.

Lee et al. in the same field of endeavor teach in response to a receipt from the mobile node of a new care- of-address that is different from a first care-of-address (“*using a newly allocated COA*”; *para. [0043]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of in response to a receipt from the mobile node of a new care- of-address that is different from a first care-of-address as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

Art Unit: 2419

Kakemizu et al. and Lee et al. do not disclose explicitly a virtual private network certificate authority.

Balaz et al. in the same field of endeavor teach explicitly a virtual private network certificate authority ("*certificate authority*"; *Abstract, Fig. 3, para. [0007], [0036], [0046], [0047]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a virtual private network certificate authority as taught by Balaz et al. One of ordinary skill in the art would be motivated to do so for providing a protocol gateway allowing routers operating in accordance with one protocol to obtain and maintain certificates for a virtual private network (VPN) from a certificate authority operating in accordance with another protocol (*as suggested by Balaz et al., see para. [0002]*).

Regarding claim 2, Kakemizu et al. disclose a network as claimed further configured to transfer context information usable by the at least first gateway in communications with the mobile node, to the second gateway (*Fig. 25, paragraphs [0114], [0115]*).

Regarding claim 3, Kakemizu et al. disclose a network as claimed wherein the context information includes an identifier of the mobile node ("*care-of-address*" interpreted as context information includes an identifier of the mobile node; *paras [0004], [0100]*).

Regarding claim 4, Kakemizu et al. disclose a network as claimed wherein the identifier is a home address of the mobile node (*"home address"; paras [0004], [0100]*).

Regarding claim 5, Kakemizu et al. disclose a network as claimed wherein the context information includes material for defining secure communication means by which information is transferable securely between the mobile node in the external portion of the network and the internal secured portion of the network, via the second gateway (*paras [0017], [0024], Fig. 2, Fig. 27*).

Regarding claim 6, Kakemizu et al. disclose a network as claimed wherein the secure communication means is a security association pair between the second gateway and the mobile node (*Fig. 27, "position registration request message (HAR), and "position registration response (HAA)" interpreted as secure communication means is a security association pair; paras [0128], [0129]*).

Regarding claim 7, Kakemizu et al. disclose a network as claimed wherein the context information is transferred from a location that is physically separate from the first gateway (*"element 23 AAAF"; Fig. 27, paras [0127], [0129]*).

Regarding claim 8, Kakemizu et al. disclose a network as claimed further configured to transfer information to the mobile node for enabling communications between the mobile node and the second gateway (*Fig. 27, para [0129]*).

Regarding claim 9, Kakemizu et al. disclose a network as claimed wherein the information transferred to the mobile node enables secure communication means by which information is transferable securely between the mobile node in the external portion of the network and the internal secured portion of the network, via the second gateway (*“elements “Reg Req 1, and Reg Rep 8 and authentication request message , AMR” interpreted as the information transferred to the mobile node enables secure communication means; Fig. 27, paras [0127]-[0129].*

Regarding claim 10, Kakemizu et al. disclose a network as claimed wherein the secure communication means is a security association pair between the mobile node and the second gateway (*Fig. 27, “position registration request message (HAR), and “position registration response (HAA)” interpreted as secure communication means is a security association pair; paras [0128], [0129].*

Regarding claim 11, Kakemizu et al. disclose a network as claimed wherein the information transferred to the mobile node comprises an address of the second gateway (*Fig. 27, para. [0128].*

Regarding claim 12, Kakemizu et al. disclose a network as claimed wherein the information transferred to the mobile node is transferred between the first gateway and the mobile node using an existing security association between the mobile node and the first gateway (*elements “Reg Req 1, and Reg Rep 8 and authentication request message , AMR” interpreted as the information transferred*

Art Unit: 2419

to the mobile node is transferred between the first gateway and the mobile node;

Fig. 27, paras [0127]-[0129]).

Regarding claims 13, 15, Kakemizu et al. disclose a network as claimed wherein the second gateway comprises one or more databases which are updated to enable the internal secured portion of the network and the mobile node in the external portion of the network to communicate via the second gateway (*"element 34 VPN database"; Fig. 27, paras [0128], [0129]).*

Regarding claim 17, Kakemizu et al. disclose a network as claimed further configured to detection means for detecting a present location of the mobile node and change gateway through which the mobile node communicates with the internal secured portion of the network, from the first gateway to a better gateway (*element 33 AAAH" interpreted as the location detection means; Fig. 25, Fig.26, paras [0119]-[0121).*

Regarding claim 18, Kakemizu et al. disclose a network as claimed wherein the better gateway is better because it is either closer to the mobile node or it is optimal for routing existing sessions (*Fig. 13, paras [0080], [0081]).*

Regarding claim 22, Kakemizu et al. disclose a network as claimed further configured to detect a present location via a location detection means that is separate from the first gateway (*"element 33 AAAH" interpreted as configured to detect a present location from a source that is separate from the first gateway (VPHGW(HA) interpreted as first gateway); Fig. 25, Fig.26, paras [0119]-[0121]).*

Regarding claim 23, Kakemizu et al. disclose a network as claimed further configured to transfer information via transfer means physically separate

Art Unit: 2419

from the first gateway and wherein the transfer means and the location detection means are housed together (*Fig. 6, paras [0071], [0072]*).

Regarding claim 24, Kakemizu et al. disclose a network as claimed wherein the first gateway and the second gateway are in distinct physically separated segments of the network (*VPNGW(FA) interpreted as first gateway which is located at roaming-contracted ISP network, and VPNGW(HA) interpreted as second gateway which is located at HOME ISP; Fig. 25, Fig. 26*).

Regarding claim 25, Kakemizu et al. disclose a network as claimed wherein the mobile node communicates with the internal secured portion of the network via the first gateway and also via the second gateway simultaneously for a transition period, before communicating via the second gateway only (*Fig. 26, paras [0120]-[0121]*).

Regarding claim 26, Kakemizu et al. disclose a network as claimed wherein the mobile node is involved in a session with a correspondent node (*para [0128]*).

Regarding claim 27, Kakemizu et al. disclose a network as claimed wherein the correspondent node is located in the internal secured portion of the network and the mobile node is located in the external portion of the network (*"CN" interpreted as correspondent node is located in the internal portion of the network; "MN 1" interpreted as the mobile node is located in the external portion of the network; Fig. 2, Fig. 26*).

Regarding claim 28, Kakemizu et al. disclose a method comprising: determining when a first serving gateway through which a mobile node

Art Unit: 2419

communicates from an external portion of a network with an internal secured portion of the network, is suboptimal (*Fig. 13, paras [0080], [0081]*); identifying a second gateway ("*reads the address of the VPNGW*"; *paras [0080], [0081]*); and in response to the mobile node moving (*Fig. 26, paras. [0119]*), and transferring the point the gateway through which the mobile node communicates with the internal portion of the network from the first serving gateway to the second gateway (*Fig. 26, paras. [0119] – [0121]*), except sending a new care-of-address that is different from a first care-of-address to the first serving gateway, and a private virtual network certificate authority.

Kakemizu et al. do not disclose explicitly sending a new care-of-address that is different from a first care-of-address to the first serving gateway.

Lee et al. in the same field of endeavor teach sending a new care-of-address that is different from a first care-of-address to the first serving gateway ("*using a newly allocated COA*"; *para. [0043]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of sending a new care-of-address that is different from a first care-of-address to the first serving gateway as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

Kakemizu et al. and Lee et al. do not disclose explicitly a virtual private network certificate authority.

Balaz et al. in the same field of endeavor teach a virtual private network certificate authority ("*certificate authority*"; *Abstract, Fig. 3, para. [0007], [0036], [0046], [0047]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a virtual private network certificate authority as taught by Balaz et al. One of ordinary skill in the art would be motivated to do so for providing a protocol gateway allowing routers operating in accordance with one protocol to obtain and maintain certificates for a virtual private network (VPN) from a certificate authority operating in accordance with another protocol (*as suggested by Balaz et al., see para. [0002]*).

Regarding claim 29, Kakemizu et al. disclose a mobile node (*Fig. 1, Fig. 2, Fig. 4*) comprising: means for receiving, via a first secure communication means, an identifier of a second gateway (*Fig. 27, paragraph [0128]*); and means for changing from communicating with the internal secured portion of the network through the first gateway to communicating via the second gateway (*Fig. 27, paragraphs [0128]-[0129]*), except in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway, and a private virtual network certificate authority.

Kakemizu et al. do not disclose explicitly in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway.

Lee et al. in the same field of endeavor teach in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway (*"using a newly allocated COA"; para. [0043]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway. as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

Kakemizu et al. and Lee et al. do not disclose explicitly a virtual private network certificate authority.

Balaz et al. in the same field of endeavor teach a virtual private network certificate authority (*"certificate authority"; Abstract, Fig. 3, para. [0007], [0036], [0046], [0047]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a virtual private network certificate authority as taught by Balaz et al. One of ordinary skill in the art would be motivated to do so for providing a protocol gateway allowing routers operating in accordance with one protocol to obtain and maintain certificates for a virtual private network (VPN) from a certificate authority operating in accordance with another protocol (*as suggested by Balaz et al., see para. [0002]*).

Regarding claim 30, Kakemizu et al. disclose a mobile node as claimed further comprising means for using a first secure communication means by which information is transferable securely between the internal portion of the network and the mobile node via the first gateway, to receive the identifier of the second gateway (*elements "Reg Req 1, and Reg Rep 8 and authentication request message , AMR" interpreted as the information transferred to the mobile node is transferred between the first gateway and the mobile node; Fig. 27, paragraphs [0127]-[0129]);*

Regarding claim 31, Kakemizu et al. discloses a mobile node as claimed further comprising means for using a second secure communication means to transfer information securely between the internal portion of the network and the mobile node via the second gateway (*Fig. 27, "position registration request message (HAR), and "position registration response (HAA)" interpreted as means for using a second secure communication means; paragraphs [0128], [0129]).*

Regarding claim 32, Kakemizu et al. disclose a method comprising: moving in an external portion of a network, where the network comprises an internal secured portion, the external portion, at least a first gateway, and at least a second gateway; obtaining a location identifier (*Fig. 27, paragraphs [0128]-[0129]*), Kakemizu et al. also disclose where the location identifier comprises a care-of-address (*"care-of-address"; para. [0100]*).

Kakemizu et al. do not disclose explicitly where the location identifier comprises a new care-of-address different from a first care-of-address; sending the new care-of-address to the first gateway; and in response to receiving an acknowledgement from the second gateway, communicating via the second gateway, and a private virtual network certificate authority.

Lee et al. in the same field of endeavor teach where the location identifier comprises a new care-of-address different from a first care-of-address; sending the new care-of-address to the first gateway; and in response to receiving an acknowledgement from the second gateway, communicating via the second gateway (*"using a newly allocated COA"; para. [0043]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of where the location identifier comprises a new care-of-address different from a first care-of-address; sending the new care-of-address to the first gateway; and in response to receiving an acknowledgement from the second gateway, communicating via the second gateway as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

Kakemizu et al. and Lee et al. do not disclose explicitly a virtual private network certificate authority.

Balaz et al. in the same field of endeavor teach a virtual private network certificate authority ("*certificate authority*"; *Abstract, Fig. 3, para. [0007], [0036], [0046], [0047]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a virtual private network certificate authority as taught by Balaz et al. One of ordinary skill in the art would be motivated to do so for providing a protocol gateway allowing routers operating in accordance with one protocol to obtain and maintain certificates for a virtual private network (VPN) from a certificate authority operating in accordance with another protocol (*as suggested by Balaz et al., see para. [0002]*).

Regarding claims 33, 34, Kakemizu et al. disclose a method and apparatus comprising and an apparatus configured to (*Fig. 1, Fig. 2, Fig. 4*): updating a location database in order to change an identification of a gateway that the mobile node uses to communicate from an external portion of the network to an internal secured portion of the network (*paras. [0113], [0119]-[0121]*), except receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network, and a private virtual network certificate authority.

Kakemizu et al. do not disclose explicitly receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network.

Lee et al. in the same field of endeavor teach receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network (*para. [0043]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

Kakemizu et al. and Lee et al. do not disclose explicitly a virtual private network certificate authority.

Balaz et al. in the same field of endeavor teach a virtual private network certificate authority ("*certificate authority*"; *Abstract, Fig. 3, para. [0007], [0036], [0046], [0047]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a virtual private network certificate authority as taught by Balaz et al. One of ordinary skill in the art would be motivated to do so for providing a protocol gateway allowing routers operating in accordance with one protocol to obtain and maintain certificates for a virtual private network (VPN) from a certificate authority operating in accordance with another protocol (*as suggested by Balaz et al., see para. [0002]*).

Art Unit: 2419

Regarding claimed 35, Kakemizu et al. disclose the network is a virtual private network ("*VPN*"; *Abstract, Fig. 1, para. [0010], Fig. 4, para. [0063]*)

4. Claims 14, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kakemizu et al. (US 20020018456 A1) and Lee et al. (US 20020085517 A1) as applied to claims 1, 13, 15 above, and further in view of Shapira et al. (US 7107464 B2).

Regarding claims 14, 16, Kakemizu et al. disclose a network as claimed wherein the second gateway comprises one or more databases ("*element 34 VPN database*"; *Fig. 27, paras [0128], [0129]*).

Kakemizu et al. and Lee et al. do not disclose explicitly wherein the one or more databases are a security policy database and a security association database.

Shapira et al. in the same field of endeavor teach wherein the one or more databases are a security policy database and a security association database ("*a security association database (SAD)*"; *col. 6, lines 47 – 54, "Security Policy Database (SPD)*"; *col. 14, lines 39 – 48*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of wherein the one or more databases are a Security Policy Database and a Security Association Database as taught by Shapira et al. One of ordinary skill in the art would be motivated to do so for providing a mechanism for implementing virtual private networks (VPNs) incorporating a security

Art Unit: 2419

association database and associated processor (*as suggested by Shapira et al., see col. 1, lines 8 – 11*).

5. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. (US 20060179298 A1) in view of Kakemizu et al. (US 20020018456 A1).

Regarding claim 36, Balaz et al. disclose a virtual private network certificate authority (Abstract, Fig. 1), comprising: means for updating a location database (*Fig. 4, Fig. 5, paras. [0053] – [0056]*); and means for forming first and second security associations with a gateway node (*paras. [0036], [0037]*), except means for forming first and second security associations with a mobile node.

Kakemizu et al. in the same field of endeavor teach means for forming first and second security associations with a mobile node (*Fig. 4, Fig. 13, paras [0080], [0081]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Balaz et al. and Lee et al. to include the features of means for forming first and second security associations with a mobile node as taught by Kakemizu et al. One of ordinary skill in the art would be motivated to do so for providing a VPN setting service that enables the communications in the mobile IP to be carried out by using a safe communication path (*as suggested by Kakemizu et al., see para. [0012]*).

Response to Arguments

6. Applicant's arguments filed on 4/21/2009 with respect to claims 1 – 9, 22 – 36 have been considered but are moot in view of the new ground(s) of rejection.

Regarding amended claims 1, applicant argues that reference Lee, like Kakemizu does not teach or suggest "an internal secured portion comprising a virtual private network certificate authority".

In response to Applicant's remark/argument, Examiner respectfully disagrees with the remark/argument addressed above since the new grounds of rejection set forth below clearly disclosed that the combined system of Kakemizu et al. and Lee et al. and Balaz et al. (newly found reference) teaches the applicant claimed invention and subject matters.

Examiner interpreted a virtual private network certificate authority as "certificate authority"; see Balaz et al. *Abstract, Fig. 3, para. [0007], [0036], [0046], [0047]*.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a) Jing et al. (US 7298847 B2).
- b) Xu et al. (US 6738362 B1).
- c) Amin et al. (US 6714987 B1).

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew C. Lee whose telephone number is

Art Unit: 2419

(571)272-3131. The examiner can normally be reached on Monday through Friday from 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew C Lee/
Examiner, Art Unit 2419
<5/07/2009::3Qy09>

/Salman Ahmed/
Examiner, Art Unit 2419